

What is claimed is:

- 1 1. A system for managing network traffic exchanged with a
2 proscribed application capable of taking evasive action, comprising:
3 a flow analyzer analyzing flow characteristics of network traffic
4 comprising a multiplicity of transient packets each including a parameterized
5 header, comprising:
6 a parser retrieving operational characteristics from the
7 parameterized header of each such transient packet generated by a plurality of
8 intercommunicating applications;
9 a comparator identifying a proscribed application by comparing the
10 operational characteristics to stored characteristics unique to the proscribed
11 application; and
12 a flow monitor controlling transmission of each such transient packet
13 subsequently exchanged with the proscribed application.
- 1 2. A system according to Claim 1, further comprising:
2 a classifier classifying a connection to the proscribed application by
3 examining connection initialization operational characteristics.
- 1 3. A system according to Claim 1, further comprising:
2 a classifier classifying a login to the proscribed application by examining
3 session initiation operational characteristics.
- 1 4. A system according to Claim 1, further comprising:
2 a classifier classifying a raw data flow to the proscribed application by
3 examining data flow operational characteristics.
- 1 5. A system according to Claim 1, further comprising:
2 a traffic manager incrementally restricting bandwidth allocated to the
3 network traffic specifically exchanged with the proscribed application until an
4 evasive action is detected.
- 1 6. A system according to Claim 5, further comprising:

2 a bandwidth restriction store recording a bandwidth restriction threshold at
3 which the evasive action by the proscribed application was triggered.

1 7. A system according to Claim 5, further comprising:
2 the traffic manager relaxing the bandwidth allocated to the network traffic
3 specifically exchanged with the proscribed application by at least one increment
4 responsive to the evasive action.

1 8. A system according to Claim 1, wherein the operational
2 characteristics comprise at least one of a network address, port and traffic
3 direction flow.

1 9. A system according to Claim 1, wherein the transient packets are
2 communicated via the TCP/IP protocol.

1 10. A method for managing network traffic exchanged with a
2 proscribed application capable of taking evasive action, comprising:
3 analyzing flow characteristics of network traffic comprising a multiplicity
4 of transient packets each including a parameterized header, comprising:
5 retrieving operational characteristics from the parameterized
6 header of each such transient packet generated by a plurality of
7 intercommunicating applications;
8 identifying a proscribed application by comparing the operational
9 characteristics to stored characteristics unique to the proscribed application; and
10 controlling transmission of each such transient packet subsequently
11 exchanged with the proscribed application.

1 11. A method according to Claim 10, further comprising:
2 classifying a connection to the proscribed application by examining
3 connection initialization operational characteristics.

1 12. A method according to Claim 10, further comprising:
2 classifying a login to the proscribed application by examining session
3 initiation operational characteristics.

1 13. A method according to Claim 10, further comprising:
2 classifying a raw data flow to the proscribed application by examining
3 data flow operational characteristics.

1 14. A method according to Claim 10, further comprising:
2 incrementally restricting bandwidth allocated to the network traffic
3 specifically exchanged with the proscribed application until an evasive action is
4 detected.

1 15. A method according to Claim 14, further comprising:
2 recording a bandwidth restriction threshold at which the evasive action by
3 the proscribed application was triggered.

1 16. A method according to Claim 14, further comprising:
2 relaxing the bandwidth allocated to the network traffic specifically
3 exchanged with the proscribed application by at least one increment responsive to
4 the evasive action.

1 17. A method according to Claim 10, wherein the operational
2 characteristics comprise at least one of a network address, port and traffic
3 direction flow.

1 18. A method according to Claim 10, wherein the transient packets are
2 communicated via the TCP/IP protocol.

1 19. A computer-readable storage medium holding code for performing
2 the method according to Claims 10, 11, 12, 13, 14, 15, 16 and 17.

1 20. A system for dynamically controlling a rogue application through
2 incremental bandwidth restrictions, comprising:
3 a flow monitor monitoring a network connection supporting a flow of
4 network traffic in a distributed computing environment, the network traffic flow
5 comprising a stream of data packets generated by a rogue application and
6 incrementally adjusting bandwidth allocated to the monitored network connection

7 until the flow of the network traffic for the rogue application achieves a steady
8 state of bandwidth restriction; and
9 a traffic manager controlling the flow of subsequent network traffic over
10 the monitored network connection at the steady state of bandwidth restriction.

1 21. A system according to Claim 20, further comprising:
2 the flow monitor decreasing the bandwidth allocated to the monitored
3 network connection for each new flow of network traffic until an evasive action
4 by the rogue application is detected.

1 22. A system according to Claim 21, further comprising:
2 the flow monitor increasing the bandwidth allocated to the monitored
3 network connection for a subsequent new flow of network traffic responsive to
4 the evasive action.

1 23. A system according to Claim 20, further comprising:
2 the flow monitor storing the steady state of bandwidth restriction as a
3 retrievable traffic flow control.

1 24. A system according to Claim 20, further comprising:
2 a flow analyzer identifying evasive action or other form of negative
3 response taken by the rogue application.

1 25. A system according to Claim 20, further comprising:
2 a flow analyzer examining at least one of a network address, port and
3 characteristics stored as parameters in a header of each such packet.

1 26. A system according to Claim 20, further comprising:
2 the flow monitor monitoring a redirected packet flow facilitated by the
3 rogue application.

1 27. A system according to Claim 20, wherein the steady state of
2 bandwidth restriction is sufficient to not trigger evasive action or other form of
3 negative response by the rogue application.

1 28. A system according to Claim 20, wherein the rogue application
2 executes in compliance with the TCP/IP protocol.

1 29. A method for dynamically controlling a rogue application through
2 incremental bandwidth restrictions, comprising:

3 monitoring a network connection supporting a flow of network traffic in a
4 distributed computing environment, the network traffic flow comprising a stream
5 of data packets generated by a rogue application;

6 incrementally adjusting bandwidth allocated to the monitored network
7 connection until the flow of the network traffic for the rogue application achieves
8 a steady state of bandwidth restriction; and

9 controlling the flow of subsequent network traffic over the monitored
10 network connection at the steady state of bandwidth restriction.

1 30. A method according to Claim 29, further comprising:
2 decreasing the bandwidth allocated to the monitored network connection
3 for each new flow of network traffic until an evasive action by the rogue
4 application is detected.

1 31. A method according to Claim 30, further comprising:
2 increasing the bandwidth allocated to the monitored network connection
3 for a subsequent new flow of network traffic responsive to the evasive action.

1 32. A method according to Claim 29, further comprising:
2 storing the steady state of bandwidth restriction as a retrievable traffic
3 flow control.

1 33. A method according to Claim 29, further comprising:
2 identifying evasive action or other form of negative response taken by the
3 rogue application.

1 34. A method according to Claim 29, further comprising:

2 examining at least one of a network address, port and characteristics stored
3 as parameters in a header of each such packet.

1 35. A method according to Claim 29, further comprising:
2 monitoring a redirected packet flow facilitated by the rogue application.

1 36. A method according to Claim 29, wherein the steady state of
2 bandwidth restriction is sufficient to not trigger evasive action or other form of
3 negative response by the rogue application.

1 37. A method according to Claim 29, wherein the rogue application
2 executes in compliance with the TCP/IP protocol.

1 38. A computer-readable storage medium holding code for performing
2 the method according to Claims 29, 30, 31, 32, 33 and 34.